

UNITED STATES DISTRICT COURT
for the
Eastern District of Michigan

United States of America

v.

Trevaughn Davorie Averitte

Case No.

Case: 2:24-mj-30228

Assigned To : Unassigned

Assign. Date : 6/13/2024

Description: COMP USA V. SEALED
MATTER (KB)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 2019 through April 2023 in the county of Macomb and elsewhere in the
Eastern District of Michigan, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 1028A, 1029(a)(3)	Aggravated Identity Theft, possession of 15 or more access devices
18 U.S.C. § 1344	Bank fraud
18 U.S.C. § 1343	Wire fraud

This criminal complaint is based on these facts:
see attached affidavit.

Continued on the attached sheet.



Complainant's signature

Michael Bertrand, Special Agent (FBI)

Printed name and title



Judge's signature

Hon. Anthony P. Patti, United States Magistrate Judge

Printed name and title

Date: June 12, 2024

City and state: Detroit, Michigan

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Michael Bertrand, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for issuance of a criminal complaint and arrest warrant for TREVAUGHN DAVORIE AVERITTE (DOB XX/XX/1993).

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so since 2022. I am currently assigned to the FBI’s Detroit Cyber Division. My current duties concern investigating crimes involving computer fraud, wire fraud, identity theft, money laundering, and conspiracies to commit those crimes. I have a Bachelor of Arts Degree in Philosophy, a Master’s Degree in Philosophy, a Doctoral Degree in Philosophy and approximately ten years of professional experience as a university philosophy professor. Additionally, I have received specialized training in the FBI relevant to the investigation of computer-related crimes.

3. This affidavit is based upon information supplied to me by other law enforcement officers, including other Special Agents employed by the FBI and Special Agents from the Department of Labor – Office of Inspector General. It is also based upon my personal involvement in this investigation and on my training and experience. In submitting this affidavit, I have not included every fact known to

me about the investigation, but instead have included only those facts that I believe are sufficient to establish probable cause to support this application for issuance of an arrest warrant.

4. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028A (Aggravated Identity Theft); 1029(a)(3) (possession of 15 or more access devices); 1344 (Bank Fraud), and 1343 (wire fraud), have been committed by TREVAUGHN DAVORIE AVERITTE.

5. The criminal activity alleged involves AVERITTE (1) purchasing user credentials sold on the cybercriminal marketplace Genesis market, (2) creating and using fraudulent identities and bank accounts, and (3) fraudulently obtaining pandemic assistance totaling \$588,481.

BACKGROUND CONCERNING GENESIS MARKET

6. Since August 2018, the FBI has been investigating an illicit online marketplace named Genesis Market.¹ Genesis Market was primarily hosted at the

¹ On April 4, 2023, the FBI and its partners dismantled Genesis Market and arrested many of its users around the world. See Department of Justice Office of Public Affairs, *Criminal Marketplace Disrupted in International Cyber Operation*, April 5, 2023, available at www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation/ (last visited 4/5/2023). Genesis Market has since resumed operation.

internet domain “genesis.market.”² Genesis Market’s operators compiled stolen data (e.g., computer and mobile device identifiers, email addresses, usernames, and passwords) from malware-infected³ computers around the globe and packaged it for sale.⁴

7. The packages advertised for sale on Genesis Market vary by price and many packages are available for around \$10 to \$20 per package. Many packages included a fingerprint for the victim computer, that is, a group of identifiers that

² A domain name is a way to identify computers on the internet, using a series of characters that correspond with a particular IP address. Genesis Market was also associated with certain backup domains in case the primary domain is shut down or taken offline for any reason. Those backup domains included the website “g3n3sis.org,” as well as the TOR domain “genesiswiwn7p7lmbvimap7v767e64rcw6o3kfcnobu3nxisteprx2qd.onion.” TOR is short for “The Onion Router” and is free, publicly available software for enabling anonymous communication over the internet. The TOR software is designed to enhance users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers around the world, thereby masking the user’s actual IP address, which could otherwise be used to identify a user.

³ Malware, or malicious software, refers to any piece of software that is written to damage and/or steal data from an internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

⁴ Genesis Market referred to these packages of stolen data as “bots” on their site; however, typically, an internet bot refers to a piece of software that runs automated tasks over the internet. Since Genesis Market’s use of the word “bot” strays from the normal meaning, the term “package” is used throughout this request.

third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. In situations where a fingerprint was associated with a package, Genesis Market provided the purchaser with a proprietary “Genesium” web browser or proprietary plugin (i.e., an internet browser extension that provides additional functionality). This proprietary browser or plugin amplifies that purchaser’s ability to control and access the package’s data and masquerade as the victim device.

8. Genesis Market users may search packages based on areas of interest (e.g., banking information, social media accounts, etc.), country of origin, price, and the date of infection (i.e., the date the victim device was infected with malware)

9. When a user purchases a package, the user receives access to all the identifiers associated with the package, including, but not necessarily limited to, device information, such as operating system, IP address, keyboard language, and time zone information, as well as access credentials, such as usernames and passwords, for compromised accounts.

10. In December 2020 and then again in May 2022, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market

database. The database included, among other things, Genesis Market's administrator logs; user logs; lists of all packages sold on the marketplace; payment transaction logs; malware used by Genesis Market administrators; and other pieces of information related to the market, including information from more than 55,000 Genesis Market user accounts.

AVERITTE'S ACTIVITY ON GENESIS MARKET

11. The Genesis Market data showed a Genesis user with login name "BJdj2158" (hereafter BJDJ) created a Genesis Market account on July 23, 2019 and provided email address nvvolen@gmail.com. Between July 2019 and September 2021, BJDJ conducted 608 searches for packages of stolen data. BJDJ searched primarily for telecommunications and bank account information from victims located in the United States. On 25 occasions between July 2019 and August 2021, BJDJ purchased a total of 2,572 stolen credentials collected in 28 packages, each package representing a compromised victim computer.⁵ 11 of 28 packages purchased by BJDJ contained user credentials for accessing banks or consumer credit information.

⁵ The smallest package purchased by BJDJ contained only 2 credentials, while the largest contained 1085. The average number of credentials in a package purchased by BJDJ was 90. In many cases, a package contained multiple credentials for the same website or resource, compromised at different times or saved in different locations.

12. On 43 occasions between July 2019 and August 2021, BJDJ downloaded fingerprints associated with packages they purchased. On 13 occasions between July 2020 and October 2021, BJDJ downloaded the Genesis Market proprietary plugin or proprietary “Genesium” browser used for masquerading as a victim device. Finally, on 13 occasions between December 2020 and October 2021, BJDJ downloaded a device fingerprint into the Genesis Market plugin or Genesium browser.

13. Genesis Market offered purchasers the opportunity to provide feedback concerning the quality of purchased packages, presumably after their use. Purchasers who offered this feedback received a credit of 5% of the purchase price of the package reviewed. Between July 2019 and August 2021, BJDJ provided 14 reviews of purchased packages.

14. Purchases made through Genesis Market are conducted using virtual currency, such as bitcoin.⁶ Before a purchase can be made, the user must first deposit a sum of virtual currency into their Genesis Market account. Between July 2019 and October 2021, BJDJ made eight bitcoin deposits to Genesis Market

⁶ Virtual currencies are digital tokens of value circulated over the internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use.

totaling \$262.13. Of these eight deposits, three deposits totaling \$152.97 were made with funds from bitcoin addresses held by cryptocurrency exchange Coinbase.

15. Coinbase deposits to BJDJ's Genesis Market account were sent from bitcoin addresses owned by a Coinbase user providing the name and address TREVAUGHN AVERITTE of 28XXX Flanders Ave., Warren, MI 48088 (28XXX Flanders Ave.) and email address averittetrevaughn@yahoo.com. AVERITTE is the sole named user associated with the Coinbase account registered to him.

16. Of the remaining five bitcoin payments BJDJ made to Genesis Market between July 2019 and October 2021

- a. Two deposits totaling \$26.40 made with funds from bitcoin by a SquareUp user providing the name and address AVERITTE of 28XXX Flanders Ave. and email address averittetrevaughn@yahoo.com. AVERITTE is the sole named user associated with this SquareUp account.

- b. One deposit totaling \$53.32 made with bitcoin sent from the account of a SquareUp user who provided the name CA.⁷ CA is known to law enforcement as a close associate of AVERITTE.
- c. One deposit totaling \$24.97 made with bitcoin sent from the account of a SquareUp user who provided the name KR. KR is known to law enforcement as a close associate of AVERITTE.
- d. A final deposit of \$8.11 funded from a cryptocurrency address not associated with any custodial cryptocurrency wallet.⁸

17. Genesis Market logs the IP addresses of its users when they perform actions like logging in to user profiles. Genesis Market login history shows that the BJDJ Genesis Account was accessed from IP address 74.199.2.222⁹ on 66 occasions between July 23, 2019 and October 16, 2019. On three occasions between July and August 2019, the BJDJ Genesis account was accessed from IP

⁷ True names of real people are abbreviated with initials. Wholly synthetic identities are listed in full.

⁸ While some cryptocurrency addresses are collected in wallets in the custody of cryptocurrency exchanges like Coinbase, others are held in so called non-custodial wallets exclusively controlled by their end users. Addresses in non-custodial wallets may be stored in various ways including with paper and pencil or on single purpose hardware devices.

⁹ An IP address is a numeric identifier assigned to devices communicating over the internet.

address 74.199.2.222 just prior to the purchase of packages of stolen credentials.

This same IP address was used to access AVERITTE's abovementioned SquareUp account just prior to BJDJ accessing Genesis Market.

18. On two occasions between August and November 2020, Genesis Market login history shows that the BJDJ Genesis Account was accessed from IP address 67.149.155.35. On August 6, 2020, the BJDJ Genesis account was accessed from IP address 67.149.155.35 just prior to the purchase of packages of stolen credentials. The day prior, on August 5, 2020, a device assigned IP address 67.149.155.35 logged into AVERITTE's Coinbase Account. As described more fully below, this same IP address was used to submit fraudulent EIDL loan applications.

19. Between June 22, 2019 and October 4, 2019, IP address 74.199.2.222 was assigned to devices that accessed the internet via a cable modem installed at the 28XXX Flanders Ave. This cable modem was installed on April 9, 2016 by WOW! at 28XXX Flanders Ave. and leased to AA. A query of commercial databases shows that AA is the mother of AVERITTE. Between July 16, 2020 and December 14, 2020, IP address 67.149.155.35 was assigned to devices that accessed the internet via a WOW! cable modem also leased to AA and installed at 28XXX Flanders Ave. between December 5, 2019 and December 16, 2020.

20. On April 4, 2023, law enforcement officers executed a search warrant at 28XXX Flanders Ave, the residence AVERITTE shares with AA. Pursuant to this warrant, law enforcement officers seized electronic devices from AVERITTE's possession including a black gaming computer, a Lenovo T430S laptop, a Lenovo T420 laptop, and four cellular phones.

21. Forensic examination of devices seized from AVERITTE's possession identified the following Genesis Market activity:

- a. Installation of the Genesis Market proprietary plugin and Genesis Market "Genesium" browser;
- b. Visits to the domain "genesis.market" as well as visits to the search page for Genesis Market together with searches for the terms "Credit Karma," "chase bank," "capital one," "experion," "gmail," "sprint," and "googlepay;"
- c. Visits to the purchase page belonging to Genesis Market;
- d. A desktop shortcut to genesis.market.
- e. Saved Chrome autofill value "BJdj2158" (the Genesis username described above).

22. On April 4, 2023, FBI Agents interviewed AVERITTE, who made the following claims:

- a. AVERITTE was unemployed but owned a company in the hospitality industry with no other employees. AVERITTE had no other sources of income;
- b. AVERITTE was the sole user of his Coinbase account;
- c. AVERITTE created an account on Genesis Market and used that account to search for credentials including credit card accounts;
- d. AVERITTE used his Genesis Market account to buy stolen credentials using cryptocurrency;
- e. AVERITTE used stolen credentials purchased on Genesis Market to gain access to victim accounts.

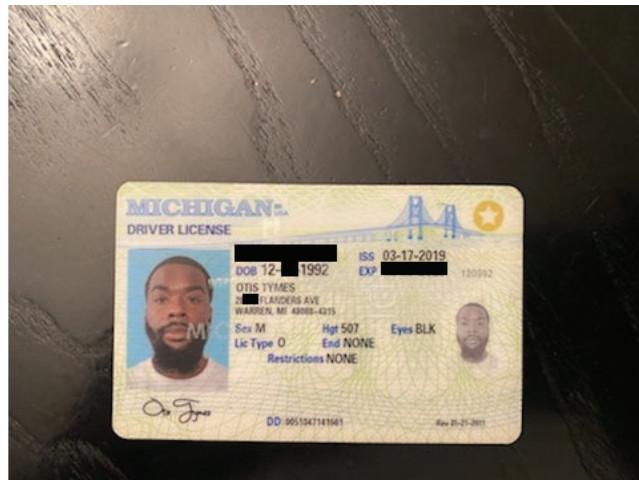
AVERITTE'S FRAUDULENT IDENTITIES AND BANK ACCOUNTS

23. Further review of physical and digital evidence seized from 28XXX Flanders Ave. revealed additional criminal activity—including possession of fraudulent identity documents, use of fraudulent bank accounts, and fraudulent applications for the Paycheck Protection Program (PPP), Economic Injury Disaster Loans (EIDL), and Pandemic Unemployment Insurance (UI) claims.

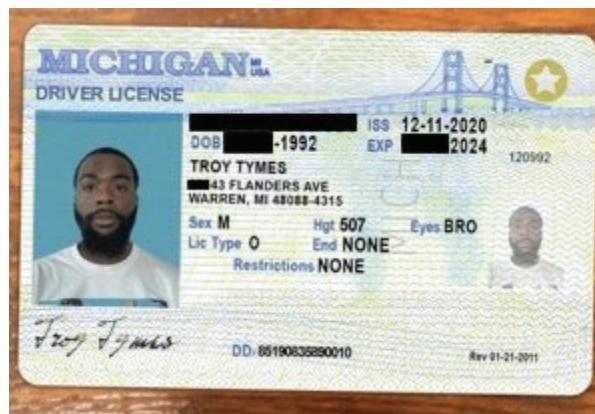
Fraudulent Identity Documents

24. The search of AVERITTE's residence and electronic devices revealed several fraudulent identities used by AVERITTE, all of which had their own false identification and Social Security cards. In some cases, the false identification

cards displayed AVERITTE's own photo. The aliases below are a sample of these fraudulent identities both possessed by AVERITTE and used to file fraudulent PPP loan applications and UI claims. The driver's licenses below were located and seized at AVERITTE's residence. In addition, images of fraudulent driver's licenses matching these aliases were discovered on AVERITTE's phones:



Otis TYMES
DOB: 12-XX-1992
SSN: XXX-XX-0255

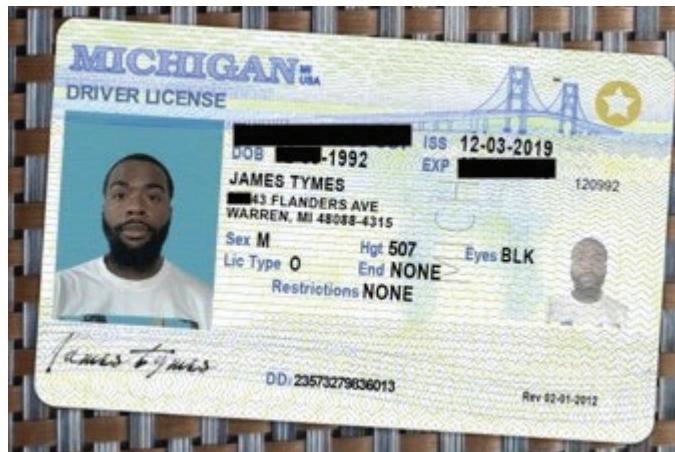


Troy TYMES
DOB: 12-XX-1992
SSN: XXX-XX-1314

25. The following photographs of fraudulent identity documents are a sample of those identified on AVERITTE's electronic devices for which no corresponding physical identifications were located. The aliases below were possessed by AVERITTE and used to file fraudulent PPP loans and bank or credit accounts under false names.



Darnell TYMES
DOB: 12-XX-1992
SSN: XXX-XX-3244



James TYMES
DOB: 12-XX-1992
SSN: XXX-XX-8724

26. Forensic investigation of AVERITTE's electronic devices also identified the following:

- a. An image of a social security card with the name Tommie Huliano. This identity was used in a fraudulent PPP loan application, more fully described below;
- b. Saved login credentials for the email account belonging to hulianotommie@gmail.com;
- c. Web browser history showing an email from authentication service ID.me addressed to hulianotommie@gmail.com;
- d. A bank statement beginning February 1, 2020 from a Huntington Bank account ending in 8234 (Huntington 8234) in the name Tommie Huliano with address 28XXX Flanders Ave. As more fully described below, Huntington 8234 received \$17,290 in fraudulent PPP loans;

27. Photographs of additional identifying documents under approximately 19 additional names were also located on AVERITTE's electronic devices.

Bank Accounts and Credit Applications

28. The search of AVERITTE's residence and electronic devices revealed bank accounts and credit applications submitted to FDIC insured financial institutions by AVERITTE under various fraudulent identities, many of which used the false names, identifications, and Social Security Numbers described above.

Some of these bank accounts were subsequently used to receive the proceeds from fraudulent PPP loans as more fully described below.

ACCOUNT HOLDER	ADDRESS	BANK	HQ	BANK ACCOUNT	FUNDS RECEIVED
Otis Tymes	28XXX Flanders Ave	Wells Fargo	San Francisco, California	Wells Fargo 8142	None identified
Otis Tymes	28XXX Flanders Ave	Huntington Bank	Columbus, Ohio	Huntington 4841	\$20,588 in fraudulent PPP loans
Darnell Tymes	28XXX Flanders Ave	Bank of America	Charlotte, NC	BoA 4034	\$40,520 in fraudulent PPP loans
Troy Tymes	28XXX Flanders Ave	Bank of America	Charlotte, NC	BoA 4157	\$20,588 in fraudulent PPP loans
Tommie Huliano	28XXX Flanders Ave	Huntington Bank	Columbus, Ohio	Huntington 8234	\$17,290 in fraudulent PPP loans

29. For each of the above accounts, the applicant provided a fraudulent SSN, date of birth, and driver's license number matching the fraudulent identity documents discussed above. The signature cards for each account were submitted via the internet to the bank in question, each of which is FDIC insured. None of the above banks are headquartered in the Eastern District of Michigan.

AVERITTE'S PPP AND EIDL LOAN FRAUD

30. The following paragraphs describe Paycheck Protection Program (PPP) loan fraud and Economic Injury Disaster Loans (EIDLs) fraud identified in digital and physical evidence seized from 28XXX Flanders Ave.

31. AVERITTE engaged in a PPP and EIDL loan fraud scheme that defrauded federal agencies and non-bank lenders of approximately \$158,788 dollars earmarked for Pandemic Assistance under the Coronavirus Aid, Relief, and Economic Securities (CARES) Act. Specifically, AVERITTE applied for at least seven fraudulent PPP loans and at least 25 fraudulent EIDL loan claims.

Background Concerning the CARES Act

32. Beginning in or about March 2020 and continuing through approximately September 2021, the Coronavirus Aid, Relief, and Economic Securities (CARES) Act created federal programs that allowed for the significant outlay of federal funds flowing to and through the states to offset the historic need for aid to businesses and their employees in the face of the COVID-19 Pandemic.

33. The CARES Act provided authorization of up to \$349 billion in forgivable loans to small businesses for job retention and certain other expenses, through a program referred to as the Paycheck Protection Program (PPP). In or around April 2020, Congress authorized over \$300 billion in additional PPP funding.

34. To obtain a PPP loan, a business had to submit a PPP loan application (SBA Form 2483), which was signed by an authorized representative of the business. The PPP loan application required the business (through its authorized representative) to acknowledge the program rules and to make certain affirmative certifications regarding its eligibility. In the application, the small business's

authorized representative also had to provide, among other things, the business's average monthly payroll expenses and number of employees. These figures were used to calculate the business's eligibility and the amount of money it may receive under the PPP. In addition, businesses applying for a PPP loan were required to provide documentation showing their payroll expenses.

35. In the course of applying for a PPP loan, the applicant must certify statements including the following:

- a. The applicant has read and understood SBA Application to include the foregoing;
- b. All loan proceeds would be used only for business-related purposes as specified in the loan application;
- c. The applicant is not engaged in any illegal activity;
- d. The applicant understands that knowingly making false statements in order to obtain a PPP loan is fraud and in violation of federal law.

36. A PPP loan application would be processed by a participating lending financial institution. If a PPP loan application was approved for funding by the participating financial institution, that institution funded the PPP loan using its own monies, which are 100% guaranteed by the SBA.

37. The PPP allowed the interest and principal on a PPP loan to be entirely forgiven if the business spent the loan proceeds on these items within a designated

period of time (usually within twenty-four weeks of receiving the proceeds) and used at least 60% of the PPP loan proceeds for payroll expenses.

38. Another component of the CARES Act was the Small Business Administration's (SBA) Economic Injury Disaster Loans (EIDLs). The SBA provided that, in response to COVID-19, EIDLs would provide economic relief to small businesses and non-profit organizations that were experiencing a temporary loss of revenue. EIDL proceeds could be used to cover a wide array of working capital and normal operating expenses, such as continuation to health care benefits, rent, utilities, and fixed debt payments. Initially, the EIDL program limited an applicant to six months of economic injury with a maximum loan amount of \$150,000. Starting the week of April 6, 2021, the SBA raised the loan limit to 24 months of economic injury with a maximum loan amount of \$500,000.

AVERITTE's Fraudulent PPP Loans

39. Seven PPP loans totaling \$138,788 were distributed to businesses listing their address as 28XXX Flanders Ave. Of these seven PPP loans, two loans totaling \$39,802 were issued in AVERITTE's name and five additional loans totaling \$98,986 were issued in the names of fraudulent identities created by AVERITTE.

PPP loans in the Name of Trevaughn AVERITTE

40. On April 4, 2021, a PPP loan was filed via the internet using AVERITTE's name and Social Security Account Number (SSN), listing address 28XXX Flanders Ave. and email averittetrevaughn@yahoo.com. The claimant certified that AVERITTE was a self-employed barber whose business is located at 28XXX Flanders Ave. No such business exists.

41. Attached electronically to the application was a photograph of AVERITTE's MI driver's license and a bank statement from a Bank of America account ending in 2929 (BoA 2929). Bank of America is insured by the FDIC. Initials and an electronic signature purporting to be AVERITTE's was affixed to the loan application via the secure document signing service DocuSign. The claimant directed funds to a Michigan First Credit Union account ending in 4770 (MFCU 4770). Michigan First Credit Union is insured by the NCUA.

42. On April 13, 2021, a \$19,901 SBA loan ending in 8803 was issued to AVERITTE from non-bank lender Fountainhead SBF LLC, headquartered in Lake Mary, FL.

43. MFCU 4770 and BoA 2929 are held in the name of AVERITTE, listing address 28XXX Flanders Ave.

44. On April 23, 2021, MFCU 4770 received a deposit of \$19,901 from Fountainhead SBF. These funds were transferred via interstate wires. In the month

of April, MFCU 4770 also received \$2,648 in Unemployment Insurance (UI) benefits and \$3,700 in Zelle transfers from Darnell Tymes, an alias used by AVERITTE and discussed above.

45. On April 13, 2021, a second PPP loan application was filed via the internet in the name, SSN, address, and email of AVERITTE. The claimant requested an additional \$19,901 PPP loan to be used for payroll expenses. The claimant directed funds to a Bank of America account ending in 2929 (BoA 2929).

46. On May 27, 2021, a \$19,901 SBA loan ending in 9003 was issued to AVERITTE from non-bank lender B.S.D Capital, Inc, doing business as Lendistry (Lendistry), headquartered in Brea, California. On June 2, 2021, an SBA loan ending in 9003 was sold to non-bank lender Harvest SBF, LLC.

47. On June, 4, 2021, BoA 2929 received \$19,901 from payee “Harvest Small Bu” with the description “Lendistry.” Account history between May 27, 2021 and June 6, 2021 also showed:

- a. \$13,000 in Zelle transfers from Darnell Tymes, a fraudulent identity used by AVERITTE;
- b. \$10,900 in Zelle transfers from Troy Tymes, a fraudulent identity used by AVERITTE;
- c. \$27,300 in cash withdrawals

PPP loans in the Name of Otis Tymes

48. On May 27, 2021, a PPP loan application was filed via the internet in the name and SSN of Otis Tymes, a fraudulent identity utilized by AVERITTE. The claimant listed address 28XXX Flanders Ave. and email address otistymes210@gmail.com. Otis Tymes' application and supporting IRS form 1040 Schedule C was substantially similar to the documents submitted by AVERITTE, listing the same occupation and gross revenue, and applying for \$20,588 to be used for payroll. Initials and an electronic signature purporting to be Otis Tymes were affixed to the loan application via DocuSign. The claimant directed funds to a Huntington Bank account ending in 5841 (Huntington 5841).

49. Forensic examination of AVERITTE's electronic devices identified an image of a MI driver's license and social security card in the name of Otis Tymes, as well as a completed IRS form 1040 Schedule C apparently matching the document submitted to in Otis Tymes' PPP loan Application.

50. On April 13, 2021, a \$20,588 SBA loan ending in 9007 was issued from non-bank lender Lendistry to Otis Tymes.

51. Huntington 5841 is held in the name of Otis Tymes, listing address 28XXX Flanders Ave.

52. On July 9, 2021, the account balance for Huntington 5841 was \$15,539. Over the course of several months, this account was depleted with a large number of

cash withdrawals and purchase such that the ending balance on November 3, 2021 was \$800.86. Between July and November 2021, only two deposits were made, totaling \$900.

PPP loans in the Name of Darnell Tymes

53. On April 17, 2021, a PPP loan application was filed via the internet in the name and SSN of Darnell Tymes, a fraudulent identity utilized by AVERITTE. The claimant listed address 28XXX Flanders Ave. and email address darnelltymes@gmail.com. Darnell Tymes' application and supporting IRS form 1040 Schedule C and applying for \$20,260 to be used for payroll.

54. In the IRS form 1040 Schedule C submitted in support of their PPP loan application, the claimant listed Darnell Tymes' address as XXX8 Stoepel, Detroit, MI. AVERITTE's Michigan Driver's License records list XXX8 Stoepel as AVERITTE's home address. This address was also found as a saved autofill value on AVERITTE's electronic devices.

55. Additional "know your customer" information was provided by the claimant including the following picture of a Michigan driver's license and selfie. AVERITTE's driver's license picture is included first for reference.





56. The claimant directed funds to a Bank of America account ending in 4034 (BoA 4034).

57. On April 26, 2021, an SBA loan ending in 8810 was issued from non-bank lender Benworth Capital Partners, headquartered in Coral Gables, Florida, to Darnell Tymes for \$20,260.

58. BoA 4034 is held in the name of Darnell Tymes, listing address 28XXX Flanders Ave.

59. On April, 26, 2021, BoA 4034 received \$20,260 from payee “BENWORTH PPP2” with the description “PPP LOANS.” Prior to this deposit, BoA 4034 had a balance of -\$9.90. Between April 26, 2021 and May 6, 2021, nine Zelle transfers were sent from this account to AVERITTE totaling \$17,600. On May 3, 2021, an additional \$2,400 in cash was withdrawn in \$800 increments across three

different transactions in three different locations in the Warren and Sterling Heights Michigan areas.

60. Between April 11, 2023 and May 8, 2023, three notices were mailed to Darnell Tymes at 28XXX Flanders Ave. notifying the borrower of non-payment of the PPP loan.

61. On May 12, 2021, a second PPP loan application was filed via the internet in the name and SSN of Darnell Tymes, again listing address 28XXX Flanders Ave. The claimant estimated \$97,250 in gross income and requested a second PPP loan of \$20,260.

62. The claimant again directed funds to a Bank of America account ending in 4034 (BoA 4034).

63. On May 27, 2021, an SBA loan ending in 8906 was issued to Darnell Tymes from non-bank lender Benworth Capital Partners.

64. BoA 4034 is held in the name of Darnell Tymes, listing address 28XXX Flanders Ave.

65. On May, 26, 2021, BoA 4034 received \$20,260 from payee “BEN CAP PP2” with the description “PPP LOANS.” Prior to this deposit, BoA 4034 had a balance of \$76.03. Between May 20 and June 7, 2021, seven Zelle transfers were sent from this account to AVERITTE totaling \$10,100 and one Zelle transfer of \$5.00 was sent to Otis Tymes.

66. Between May 28, 2021 and June 7, 2021, an additional \$9,000 in cash was withdrawn in \$1,000 increments across nine different transactions in different locations in the Warren and Sterling Heights Michigan areas. Of these, four transactions occurred on the same day.

67. On July 12, 2023, the Small Business Administration agreed to purchase SBA loan ending in 8906 from Benworth Capital after non-payment from Darnell Tymes. According to this purchase agreement, SBA loan ending in 8906 was in default as of September 26, 2022.

PPP loans in the Name of Troy Tymes

68. On April 23, 2021, a PPP loan application was filed via the internet in the name and SSN of Troy Tymes, a fraudulent identity utilized by AVERITTE. The claimant listed address 28XXX Flanders Ave. and email address troytymes@gmail.com. Troy Tymes's application and supporting IRS form 1040 Schedule C, applying for \$20,588 to be used for payroll. The claimant also provided the following picture of a Michigan driver's license and selfie:



69. Forensic examination of electronic devices seized from AVERITTE's residence identified a photograph of a Michigan driver's license resembling the one above as well as a completed IRS form 1040 Schedule C in the name of Troy Tymes.

70. The claimant directed funds to a Bank of America account ending in 4157 (BoA 4157).

71. On May 27, 2021, an SBA loan ending in 8900 was issued from non-bank lender Benworth Capital Partners to Troy Tymes for \$20,588.

72. BoA 4157 is held in the name of Troy Tymes, listing address 28XXX Flanders Ave.

73. On May, 26, 2021, BoA 4157 received \$20,588 from payee “BENWORTH PPP2” with the description “PPP LOANS.” Prior to this deposit, BoA 4157 had a balance of -\$14.85. Between May 27, 2021 and June 7, 2021, five Zelle transfers were sent from this account to AVERITTE totaling \$10,900. Between May 28, 2021 and June 7, 2021, an additional \$9,010 in cash was withdrawn in \$1,000 increments across nine different transactions.

74. On July 12, 2023, the Small Business Administration agreed to purchase SBA loan ending in 8900 based on the Benworth Capital after non-payment from Troy Tymes.

PPP loans in the Name of Tommie Huliano

75. On April 25, 2021, a PPP loan application was filed via the internet in the name and SSN of Tommie Huliano, a fraudulent identity utilized by AVERITTE. The claimant listed address 28XXX Flanders Ave. and email address hulianotommie@gmail.com. Huliano’s application and supporting IRS form 1040 Schedule C claimed \$83,000 in gross income from a sales business located at 28XXX Flanders Ave. and applied for \$17,290 for payroll, rent, and utilities.

76. The claimant directed funds to Huntington 8234 (as previously described, login credentials and a bank statement for this account were located on AVERITTE's electronic devices). Huntington 8234 is held in the name of Tommie Huliano, listing address 28XXX Flanders Ave.

77. On May 27, 2021, an SBA loan ending in 8905 was issued from non-bank lender Prestamos CDFI, LLC to Tommie Huliano for \$17,290.

78. On June, 2, 2021, Huntington 8234 received \$17,290 from payee "PRESTAMOSCDFIPPPFUNDING."

79. On November 2, 2021, a PPP loan forgiveness application was submitted to the Small Business Administration for the amount of \$17,290. On November 9, 2021, the Small Business Administration agreed to forgive the full balance of this loan.

AVERITTE's Fraudulent EIDL loans

80. 24 unsuccessful EIDL loan applications were submitted from devices using IP addresses also seen accessing AVERITTE's bank accounts and loan applications.

81. On August 2, 2020, a successful EIDL application ending in 2362 was submitted via the internet from IP address 67.149.155.35 in the name JR. As described above, this same IP address was leased to AA of 28XXX Flanders and accessed AVERITTE's Genesis Market and Coinbase accounts.

82. On August 3, 2020, \$20,000 was dispersed to a BancCorp account in the name of JR. BancCorp is FDIC insured. In light of AVERITTE's prolific use of fraudulent identities, it is likely that AVERITTE was the ultimate beneficiary of the EIDL application ending in 2362.

AVERITTE'S UNEMPLOYMENT INSURANCE FRAUD

83. A search of AVERITTE's electronic devices yielded evidence of Pandemic Unemployment Insurance (UI) fraud.

Background Concerning Unemployment Insurance

84. The Social Security Act of 1935 initiated the federal and state Unemployment Insurance (UI) system. The system provides benefits to individuals who are unemployed for reasons beyond their control. In the State of Michigan, the UI system is administered by the Unemployment Insurance Agency, which is part of the State of Michigan's Department of Labor and Economic Opportunity.

85. State unemployment systems and benefits are joint state and federal enterprises largely financed by taxes on private employers located in that state. In 2020 and 2021, the federal government provided significant supplemental benefits to the states as a result of the COVID-19 Pandemic. Beginning in or about March 2020 and continuing through September 4, 2021, the Families First Coronavirus Response Act; Coronavirus Aid, Relief, and Economic Security Act; and the American Rescue Plan Act of 2021 created federal programs that allowed for the

significant outlay of federal funds flowing to and through the states to offset the historic need for unemployment benefits by the American workforce, including in the State of Michigan and in the Eastern District of Michigan. Collectively, these benefits are often referred to as Pandemic Unemployment Assistance.

86. Normally (in the absence of fraud), an unemployed worker initiates a UI claim. This can be accomplished by submitting a claim in person, over the telephone, or via the internet. Currently, most UI claims are filed online via the internet through the Unemployment Insurance Agency's website. To be eligible for UI benefits, the worker must demonstrate a certain level of earnings in several quarters immediately preceding the application. The amount of benefits that an UI claimant might be eligible for depends on a variety of factors, including but not limited to the length of his or her previous employment and the amount of wages he or she earned.

87. When an individual files a claim, he or she is required to provide his or her residential address, as well as a form of official identification, such as a driver's license or government-issued identification card.

88. In the State of Michigan, the Unemployment Insurance system is administered by the Unemployment Insurance Agency (MUIA), which is part of the State of Michigan's Department of Labor and Economic Opportunity. In the State of California, the UI system is administered by the Employment Development

Department (EDD). These State Workforce Agencies (SWAs) will either approve or reject a UI claim based on the application made by the unemployed worker. If the SWA approves a UI claim, the claimant is required to re-certify the claim via telephone or internet at various times during the life of the claim. The worker must also certify that he or she is still unemployed and actively seeking work.

89. One way in which unemployment benefits are provided to a claimant is with a debit card, issued by the Bank of America (BoA), which is mailed to the claimant through the U.S. Postal Service. The agency places money on the card through an electronic transfer. Alternatively, a claimant can provide the state Unemployment Insurance Agency with a bank routing number and bank account number so his or her UI benefits can be transferred via electronic funds transfers (EFTs) into his or her bank account. These EFTs originate from one or more accounts maintained by MUIA, or EDD at Bank of America, N.A., which is a subsidiary of Bank of America Corporation, a bank holding and financial holding company headquartered in Charlotte, North Carolina. All EFTs of UI benefits to Michigan Unemployment Insurance claimants, whether via a BoA-provided debit card or via a claimant-provided bank account, involve the transmission of electronic signals through one of BoA's two data centers, which are located in Virginia and Colorado, and from those data centers to banks located in Michigan. These EFTs therefore constitute interstate wire communications.

AVERITTE's Fraudulent UI Claims

90. AVERITTE engaged in an UI fraud scheme that defrauded multiple states of approximately \$429,693 dollars that was earmarked for Pandemic Unemployment Assistance. AVERITTE is associated with over 50 suspected fraudulent UI claims, a large portion of which were filed using his own residential mailing address, 28XXX Flanders Ave.

UI Claim in Name of Trevaughn AVERITTE

91. On August 25, 2021, a California UI claim was filed in the name, SSN, and DOB of AVERITTE. The address listed by the claimant was “28XXX Flanders Ave.” The email address listed by the claimant as “AVERITTETREVAUGHN@yahoo.com” The phone number listed by the claimant was “586-XXX-9010.” According to law enforcement databases, there is no record of AVERITTE having ever lived or worked in the State of California.

UI Claims in Name of Otis Tymes, Darnell Tymes, and Troy Tymes

92. The following UI claims were filed in the names, dates of birth, and SSN’s of false identities used by AVERITTE as described above:

NAME	ADDRESS	EMAIL	SSN	PHONE	STATE FILED	DATE FILED
Otis Tymes	28XXX Flanders Ave	OTISTYMES210@gmail.com	XXX -XX- 0255	248-XXX-2575	MI	May 26, 2020
Otis Tymes	28XXX Flanders Ave	OTISTYMES210@gmail.com	XXX -XX- 0255	248-XXX-2575	PA	May 30, 2020

Otis Tymes	28XXX Flanders Ave	OTISTYMES210@gmail.com	XXX -XX- 0255	248-XXX- 2575	LA	June 18, 2020
Otis Tymes	28XXX Flanders Ave	CRYAN2159@GMAIL.COM	XXX -XX- 0255	248-XXX- 2575	CA	July 22, 2020
Otis Tymes	28XXX Flanders Ave		XXX -XX- 6648	248-XXX- 2575	CA	August 7, 2020
Otis Tymes	28XXX Flanders Ave	OTISTYMES210@gmail.com	XXX -XX- 0255	248-XXX- 2575	MT	August 12, 2020
Otis Tymes	28XXX Flanders Ave	OTISTYMES210@gmail.com	XXX -XX- 0255	248-XXX- 2575	Guam	August 13, 2020
Otis TYMES	28XXX Flanders Ave	OTISTYMES210@gmail.com	XXX -XX- 0255	248-XXX- 2575	WV	October 16, 2020
Otis Tymes	28XXX Flanders Ave	OTISTYMES210@gmail.com	XXX -XX- 6648	248-XXX- 2575	CA	August 25, 2021
Darnell Tymes	28XXX Flanders Ave		XXX -XX- 3244	586-XXX- 8808	CT	July 6, 2020
Darnell Tymes	28XXX Flanders Ave	DARNELLYMES@gmail.com	XXX -XX- 3244	586-XXX- 8808	MT	August 12, 2020
Darnell Tymes	28XXX Flanders Ave	DARNELLYMES@gmail.com	XXX -XX- 3244	586-XXX- 8808	PA	October 8, 2020
Troy Tymes	28XXX Flanders Ave		XXX -XX- 1314		CT	June 29, 2020
Troy Tymes	28XXX Flanders Ave	TROYTYMES@gmail.com	XXX -XX- 1314		CA	August 24, 2020

Additional UI Claims Associated with AVERITTE

UI Claim in Name of J.W.

93. On August 25, 2020, a California UI claim was filed in the name, SSN, and DOB of J.W., a real person. The email address listed by the claimant was “J****2101@protonmail.com.” The address listed by the claimant was “28XXX Flanders Ave.”

94. On or around August 27, 2020, a BoA UI debit card ending in 6611 in J.W.’s name was mailed, via USPS, to 28XXX Flanders Ave.” On August 28, 2020, \$19,880 was deposited into the debit account, established by the California EDD, in J.W.’s name.

95. A search of AVERITTE’s cellular devices revealed a stored screenshot image dated September 5, 2020 of a California EDD BoA debit card account in J.W.’s name. The email address on the account is listed as “J****2101@protonmail.com.”

96. BoA provided ATM surveillance footage of withdrawals made from the UI debit account set up in J.W.’s name on September 20, 2020 and September 24, 2020 in the Eastern District of Michigan. Based on a review of the ATM surveillance images, agents concluded that the individual in the ATM surveillance footage is AVERITTE. The image below shows AVERITTE making the withdrawal on September 20, 2020.



97. On December 18, 2023, agents interviewed J.W. via phone. J.W. stated that s/he did not file a UI claim in California, had not received any UI benefits, and did not give permission to anyone to file a UI claim on her/his behalf.

UI Claim in Name of J.K.

98. On January 11, 2021, a New York UI claim was filed in the name, SSN, and DOB of J.K., a real person. The email address listed by the claimant was “J*****K***210@gmail.com.” The address listed by the claimant was “3XX E 56th St. New York, NY 10022.” The phone number listed by the claimant was “586-XXX-7416.” The direct deposit bank account information provided by the claimant was for an account ending in #1245 at Green Dot Bank.

99. Records provided by Green Dot Bank revealed that account ending in #1245 belongs to AVERITTE's aliases, Otis Tymes and Troy Tymes. The address registered on the account is 28XXX Flanders Ave.

100. From January 14, 2021 to August 26, 2021, account number #1245 received 68 UI deposits from the State of New York in J.K.'s name for a total of \$27,240.

101. On January 2, 2024, agents interviewed J.K. via phone. J.K. stated that s/he did not file a UI claim in New York, had not received any UI benefits, and did not give permission to anyone to file a UI claim on her/his behalf.

28XXX Flanders Ave. Fraud Indicators

102. A DOL-OIG database query also revealed that 28XXX Flanders Ave., was listed as the mailing address on approximately 50 UI claims, including the 15 claims listed above in AVERITTE's own name and those of his aliases, filed in 12 separate states to include: one claim in Arizona, 30 claims in California, two claims in Connecticut, one claim in Guam, one claim in Louisiana, five claims in Michigan, two claims in Montana, one claim in Nevada, three claims in New York, two claims in Pennsylvania, one claim in Texas, and one claim in West Virginia. Searches in law enforcement databases reveal that most of the SSNs associated with these claims match the names of the purported claimants, thus they appear to be real people whose identities have been compromised.

103. Approximately \$400,845 in UI benefits was disbursed to claims that listed “28XXX Flanders Ave.” as the claimant’s address.

CONCLUSION

104. Based on the forgoing, there is probable cause to believe that Trevaughn AVERITTE has committed violations of 18 U.S.C. §§ 1028A (Aggravated Identity Theft); 1029(a)(3) (possession of 15 or more access devices); 1344 (Bank Fraud), and 1343 (wire fraud).

Respectfully submitted,



Special Agent Michael Bertrand
FBI

Sworn to before me and signed in my presence and/or by reliable electronic means.



Hon. Anthony P. Patti
United States Magistrate Judge

Dated: June 12, 2024